



TECHNOLOGICKÉ
CENTRUM PRAHA

HORIZONT EVROPA VÝZVY 2025 V OBLASTI KYBERNETICKÁ BEZPEČNOST

28. srpna 2025
Lenka Švejcarová



EUROPEAN UNION

#HorizonEU

HORIZON EUROPE

PILLAR 1 EXCELLENT SCIENCE

EUROPEAN RESEARCH
COUNCIL

MARIE SKŁODOWSKA-CURIE
ACTIONS

RESEARCH
INFRASTRUCTURES

PILLAR 2 GLOBAL CHALLENGES AND EUROPEAN INDUSTRIAL COMPETITIVENESS

CLUSTERS

- 1 HEALTH
- 2 CULTURE, CREATIVITY
AND INCLUSIVE SOCIETY
- 3 CIVIL SECURITY FOR SOCIETY
- 4 DIGITAL, INDUSTRY AND SPACE
- 5 CLIMATE, ENERGY AND MOBILITY
- 6 FOOD, BIOECONOMY, NATURAL
RESOURCES, AGRICULTURE AND
ENVIRONMENT

JOINT RESEARCH CENTRE

PILLAR 3 INNOVATIVE EUROPE

EUROPEAN INNOVATION
COUNCIL

EUROPEAN INNOVATION
ECOSYSTEMS

EUROPEAN INSTITUTE
OF INNOVATION
AND TECHNOLOGY

WIDENING PARTICIPATION AND STRENGTHENING THE EUROPEAN RESEARCH AREA

WIDENING PARTICIPATION AND SPREADING EXCELLENCE

REFORMING AND ENHANCING THE EUROPEAN R&I SYSTEM

Výzvy 2025 najdete ve [Funding Tenders portálu](#).

Výzvy 2026 - 2027 najdete v [registru Evropské komise](#) od str. 141. Pozor, draft!

Financované projekty najdete v portálu [CORDIS](#).



6 témat 2025 v Klastru 3 v oblasti kybernetická bezpečnost

Název tématu	Kód tématu a hyperlink	Typ projektu a financování od E.Komise	Rozpočet na každý projekt	Počet projektů k financování	Uzávěrka
Generative AI for Cybersecurity applications	HORIZON-CL3-2025-02-CS-ECCC-01	RIA (100%)	12-14 mil. EUR	max 3	12/11/2025
New advanced tools and processes for Operational Cybersecurity	HORIZON-CL3-2025-02-CS-ECCC-02	IA (100% / 70%)	4,6 - 6 mil. EUR	max 4	12/11/2025
Privacy Enhancing Technologies	HORIZON-CL3-2025-02-CS-ECCC-03	RIA (100%)	3 - 4 mil. EUR	max 3	12/11/2025
Security evaluations of Post-Quantum Cryptography (PQC) primitives	HORIZON-CL3-2025-02-CS-ECCC-04	RIA (100%)	2 - 3 mil. EUR	max 2	12/11/2025
Security of implementations of Post-Quantum Cryptography algorithms	HORIZON-CL3-2025-02-CS-ECCC-05	RIA (100%)	2 - 3 mil. EUR	max 2	12/11/2025
Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols	HORIZON-CL3-2025-02-CS-ECCC-06	RIA (100%)	2 - 3 mil. EUR	max 2	12/11/2025





7 témat 2026 - 2027 v Klastru 3 - cybersecurity

Název tématu	Typ projektu a financování od E.Komise	Rozpočet na každý projekt	Počet projektů k financování	Uzávěrka
Approaches and tools for security in software and hardware development and assessment	<i>RIA (100%)</i>	3 - 5 mil. EUR	<i>max 4</i>	<i>září 2026</i>
Enhancing the Security, Privacy and Robustness of AI Models and Systems (SecureAI)	<i>IA (100% / 70%)</i>	3 - 5 mil. EUR	<i>max 4</i>	<i>září 2026</i>
Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations	<i>RIA (100%)</i>	3 - 5 mil. EUR	<i>max 3</i>	<i>září 2026</i>
Artificial Intelligence for Cybersecurity applications	<i>RIA (100%)</i>	3 - 5 mil. EUR	<i>max 4</i>	<i>září 2027</i>
Secure Computing Continuum (IoT, Edge, Cloud, Data spaces)	<i>IA (100% / 70%)</i>	3 - 5 mil. EUR	<i>max 5</i>	<i>září 2027</i>
Secure PQC implementations, Cryptanalysis and Post-quantum Digital Trust	<i>RIA (100%)</i>	4 – 5,5 mil. EUR	<i>max 3</i>	<i>září 2027</i>
New primitives for functionalities of future hybrid quantum-classical and quantum networks	<i>RIA (100%)</i>	4 mil. EUR	<i>max 1</i>	<i>září 2027</i>



Draft výzev je [registru Evropské komise](#) od str. 141. **Pozor, bude se měnit.**



CS-ECC-01 Generativní AI pro aplikace v oblasti kybernetické bezpečnosti

HORIZON-CL3-2025-02-CS-ECCC-01: Generative AI for Cybersecurity applications

- Zaměření: Vývoj technologií, nástrojů a procesů, které posílí kybernetickou bezpečnost prostřednictvím komponent umělé inteligence, zejména generativní AI, v souladu s příslušnými politikami EU, právními a etickými požadavky.
- Výběr jedné *nebo obou variant*:
 - A) Vývoj, trénink a testování modelů genAI pro: *(i)* monitorování, detekci a reakci na kybernetické útoky (vč. AI útočníka), jakož i schopnost samo-opravy digitálních systémů, *(ii)* samo-adaptaci reakčních nástrojů dosud prováděnou ručně, *(iii)* zabránění neoprávněným přístupům a krádežím přihlašovacích údajů
 - B) Vývoj nástrojů založených na genAI, které: *(i)* analyzují a usnadní zapracování národní a evropské legislativy (AI Act NIS2 ..) do digitálních systémů, *(ii)* umožní organizacím průběžně zvládat jak regulatorní požadavky (dodržování předpisů), tak aktualizace interních ICT systémů – obojí zároveň proto, aby se o tento soulad již nemusel už starat pouze „člověk“.
- Povinní účastníci: NE
- Reflexe politik, aktivit, dosavadních projektů: [Trustworthy and Responsible AI Principles](#), [Data Spaces](#), [EOSC](#), atd.
- 12 - 14 mil. € na projekt, 3 projekty budou financovány (*min. 2 z varianty A a 1 z varianty B*); celkový rozpočet tématu 40 mil. €
- RIA; TRL neurčeno; **omezení účasti – pouze entity z EU zemí a Asociovaných zemí nekontrolované entitami z nezpůsobilých zemí; uzávěrka 12. 11. 2025**





CS-ECC-02 Nové pokročilé nástroje a procesy pro provozní kyberbezpečnost

HORIZON-CL3-2025-02-CS-ECCC-02: New advanced tools and processes for Operational Cybersecurity



- Zaměření: Předvést praktické využití vyvinutých rámců (frameworks), nástrojů, služeb a procesů formou pilotních ověření v praxi. Projekty musí být postaveny na použitelnost vyvinutých řešení.
- Výběr alespoň dvou ze šesti směrů:
 - Lepší přehled o hrozbách díky pokročilému kybernetickému zpravodajství a analýze rizik evropských dodavatelských řetězců
 - Rámce, nástroje a služby pro zvládání hybrid. a kybernet. útoků na ICT a OT infrastruktury (operational technology), simulace v praxi
 - Rozšíření schopností SOC/CSIRT týmů prostřednictvím pokročilých nástrojů pro detekci, analýzu, reakci a nápravu incidentů
 - Vývoj test. a exp. prostředí pro nové (provozní) nástroje a procesy; vytvoření digitálních dvojčat pro CI a entity* definované v NIS2
 - Vývoj RÁMCŮ a služeb pro krizové řízení a jejich odzkoušení v praxi – napříč státy a napříč různými odvětvími
 - Nastavení funkčních mechanismů pro provozní propojení veřejných bezpeč. struktur ([CSIRT network](#), [EU-CyCLONE](#), NIS2 subjektů,...)
- Doporučení účastníci: Národní úřady pro kybernetickou bezpečnost*; přední **Start-upy a SMEs**: aktivní v cybersec projektech z programů Horizont Evropa / Digitální Evropa; nebo aktivně spolupracující s národními úřady* či jinak činné v provozní kyberbezpečnosti. **Firmám doporučeno přímo koordinovat projekt, nebo vést pilotní provoz.**
- Reflexe politik, aktivit, dosavadních projektů: [Common Security Advisory Framework \(CSAF\)](#); [Cyber Solidarity Act](#); [NIS2](#); atd.
- 4.5 - 6 mil. € na projekt, 4 projekty budou financovány; celkový rozpočet tématu 23,55 mil. €
- IA; TRL alespoň 7; **omezení účasti** – pouze entity z EU zemí a Asociovaných zemí nekontrolované entitami z nezpůsobilých zemí; [lumpsum](#); **uzávěrka 12. 11. 2025**





CS-ECC-03 Technologie pro ochranu soukromí

HORIZON-CL3-2025-02-CS-ECCC-03: Privacy Enhancing Technologies (PETs)

- Zaměření: Ochrana soukromí a osobních údajů při současném umožnění zpracování a analýzy těchto údajů. Bezpečné využívání citlivých i průmyslových dat včetně odolnosti vůči kvantovým hrozbám.
- Výběr některých nebo všech směrů:
 - Vývoj robustních, škálovatelných a spolehlivých technologií, které ochrání soukromí při sdílení a zpracování dat mezi více organizacemi
 - Vývoj takových řešení, která při sdílení dat ochrání nejen citlivá data, ale i informace o kyberhrozbách a citlivých výpočtech
 - Integrace ochrany soukromí do návrhu softwaru a do protokolů s důrazem na připravenost kryptografie na post-quantové algoritmy
 - Vývoj technologií chránících soukromí i pro uživatele takových zařízení, která mají např. výpočetní limity či nízkou energetickou kapacitu
 - Přínosy pro evropské [Data Spaces](#) při zohlednění GDPR, návaznost na vyvinutá řešení v projektech HORIZON-CL4-DATA
 - Řešení vzcházející přímo z potřeb uživatelů, tj. firem (SMEs) a občanů
 - Vývoj blockchainových a decentralizovaných technologií zajišťujících důvěrnost a autenticitu dat, vč. propojení s federativním učením
 - Nejen bezpečné, ale i uživatelsky a designově přívětivé technologie
- Doporučení účastníci: průmyslové firmy, SMEs, poskytovatelé služeb, koneční uživatelé, odborníci na regulatorní překážky
- 3 - 4 mil. € na projekt, 3 projekty budou financovány; celkový rozpočet tématu 11 mil. €
- RIA; TRL neuvedeno; [omezení účasti \(čl. 22\)](#); [lumpsum](#); [uzávěrka 12. 11. 2025](#)





CS-ECC-04 Bezpečnostní analýzy základních prvků (primitiv) post-quantové kryptografie

HORIZON-CL3-2025-02-CS-ECCC-04: Security evaluations of Post-Quantum Cryptography (PQC) primitives

- Zaměření: hodnocení bezpečnosti PQC prvků prostřednictvím výzkumu kvantových algoritmů (s případným využitím AI), které přispějí k odhalení zranitelností a k návrhu robustních kryptosystémů odolných vůči budoucím kvantovým a AI řízeným útokům.
- Výběr některých nebo všech směrů:
 - Průlomové poznatky o kvantové složitosti různých tříd matematických problémů klíčových pro bezpečnost současných i post-quantových kryptosystémů
 - Kvantové algoritmy nové generace zaměřené na řešení problémů využívaných v kryptografii, jako jsou mřížky nebo kódy
 - Efektivní nasazení kvantových algoritmů s využitím kvantových programovacích jazyků v oblasti kryptografie
 - Vybudování prostředí pro zátěžové testy kryptosystémů vůči kvantovým útokům
 - Přístupy založené na AI k identifikaci zranitelností v mřížkových nebo jiných matematických strukturách
 - Výsledky kryptoanalýz
 - Návrhy parametrů pro vytvoření robustní sady kryptografických komponent pro post-quantové kryptosystémy, které budou odolné vůči kvantovým i AI útokům
- 2 - 3 mil. € na projekt, 2 projekty budou financovány; celkový rozpočet tématu 4 mil. €
- RIA; TRL neuvedeno; omezení účasti: pouze entity ze zemí EU / Asociovaných / OECD nekontrolované entitami z nezpůsobilých zemí; lumpsum; uzávěrka 12. 11. 2025





CS-ECC-05 Bezpečnost nasazení post-kvantových kryptografických algoritmů

HORIZON-CL3-2025-02-CS-ECCC-05: Security of implementations of Post-Quantum Cryptography algorithms

- Zaměření: Návrhy a ověření efektivních a nákladově únosných ochranných mechanismů proti implementačním útokům na post-kvantové šifrování, včetně útoků založených na AI. Vývoj metod pro jejich automatizované testování v reálných hardwarových a softwarových prostředích.
- Výběr některých nebo všech směrů:
 - Vývoj a praktické nasazení PQC kryptografických algoritmů odolných proti útokům typu side-channel a dalších
 - Návrh účinných protiopatření se zohledněním nejen bezpečnosti, ale i rozumných nákladů a nesnižování provozního výkonu
 - Návrh účinných protiopatření vůči širokému spektru útoků; specifikování požadavků na potřebný HARDWARE
 - Analyzování nových útoků nebo kombinovaných útoků, včetně těch s využitím AI, v kontextu praktického nasazení
 - Vývoj nástrojů pro automatické vyhodnocování bezpečnostních aspektů PQC (praktické aplikace)
- 2 - 3 mil. € na projekt, 2 - 3 projekty budou financovány; celkový rozpočet tématu 6 mil. €
- RIA; TRL neuvedeno; omezení účasti: pouze entity ze zemí EU / Asociovaných / OECD nekontrolované entitami z nezpůsobilých zemí; lumpsum; uzávěrka 12. 11. 2025





CS-ECC-06 Integrace post-kvantových kryptografických algoritmů do high-level protokolů

HORIZON-CL3-2025-02-CS-ECCC-06: Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols

- Zaměření: Migrace běžně používaných kryptografických protokolů na post-kvantové varianty protokolů, ideálně ve spolupráci výzkumných institucí, veřejného sektoru a průmyslu, pro zajištění jejich praktické využitelnosti. Doporučeno testování v nejrozumnějších aplikacích.
- Výběr některých nebo všech směrů:
 - Návrh a nasazení alespoň jednoho high-level post-kvantového protokolu, včetně bezpečnostní analýzy prokazující zachování bezpečnostních vlastností vstupních kryptografických prvků
 - Zajištění přenosu takto vyvinutých PQC protokolů do praxe prostřednictvím standardizačních organizací a/nebo pomocí open-source projektů
 - Analýza požadavků (vč. překážek) nutných k plnému přechodu high-level protokolů do PQC
- Doporučení účastníci: výzkumné organizace, relevantní veřejné instituce, průmyslové subjekty
- 2 - 3 mil. € na projekt, 2 - 3 projekty budou financovány; celkový rozpočet tématu 6 mil. €
- RIA; TRL neuvedeno; omezení účasti: pouze entity ze zemí EU / Asociovaných / OECD nekontrolované entitami z nezpůsobilých zemí; lumpsum; uzávěrka 12. 11. 2025



Kaskádové granty

HORIZONT EVROPA & DIGITÁLNÍ EVROPA

Příjemce podpory, tj. projektové konsorcium, vyhlásí v průběhu realizace projektu vlastní výzvy k podávání návrhů, tzv. **open calls**.

Oprávněnými žadateli jsou převážně jednotlivé malé a střední podniky, nebo malá konsorcia různých typů organizací.

Jedná se o grantové částky obvykle **do 100 tisíc €** a experimenty s dobou realizace menší než **1 rok**. Tato finanční podpora **třetích stran** formou grantů je označována též jako **Financial support to third parties (FSTP)**.



[Seznam](#) Open Calls ve
Funding & Tenders Portálu

European Commission | EU F&T Portal

Sign in EN

Home > Funding > Calls for proposals

Calls for proposals

Calls for proposals are funding opportunities issued by the European Union institutions, agencies and bodies. These are direct financial contributions, known as grants, that are awarded to third-party beneficiaries (e.g., research organisations, public entities, non-governmental organisations, and private companies) to engage in activities that serve EU policies.

[More details](#)

Filters

Quick search

quantum

2021 - 2027

Programme

Call

Submission status

All filters

GRANTS RECOMMENDED FOR YOU

Do you want to receive personalised recommendations? [Log in](#) to your F&T profile or [register](#) an account to activate them.

4 item(s) found

CyberSecDome Open Call - Round 2

CyberSecDome | Cascade funding

Opening date: 01 August 2025 | Deadline date: 30 September 2025 ...

Programme: Horizon Europe (HORIZON) | Type of action: -

DTU Open Call

DigiWind | Cascade funding

Opening date: 15 August 2025 | Deadline date: 15 October 2025 | ...

Programme: Digital Europe Programme (DIGITAL) | Type of action: -

Second call for innovation studies for the development of generat...

FFplus | Cascade funding

Opening date: 10 September 2025 | Deadline date: 26 November 2025 | Sing...

Programme: Digital Europe Programme (DIGITAL) | Type of action: -



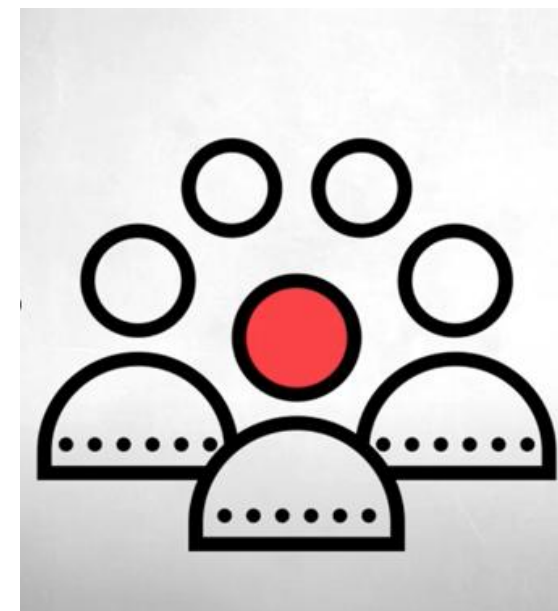
JAK SE ZAPOJIT NA POSLEDNÍ CHVÍLI?



1. Obraťte se na Lenku Švejcarovou, národní kontakt pro ČR. 
2. Vyberte si vhodnou výzvu a popište vůči výzvě svůj inovativní záměr. 
3. Najděte konsorcium a nabídněte jim svůj záměr. Kde hledat?

Oslovováním svých mezinárodních kontaktů, nebo:

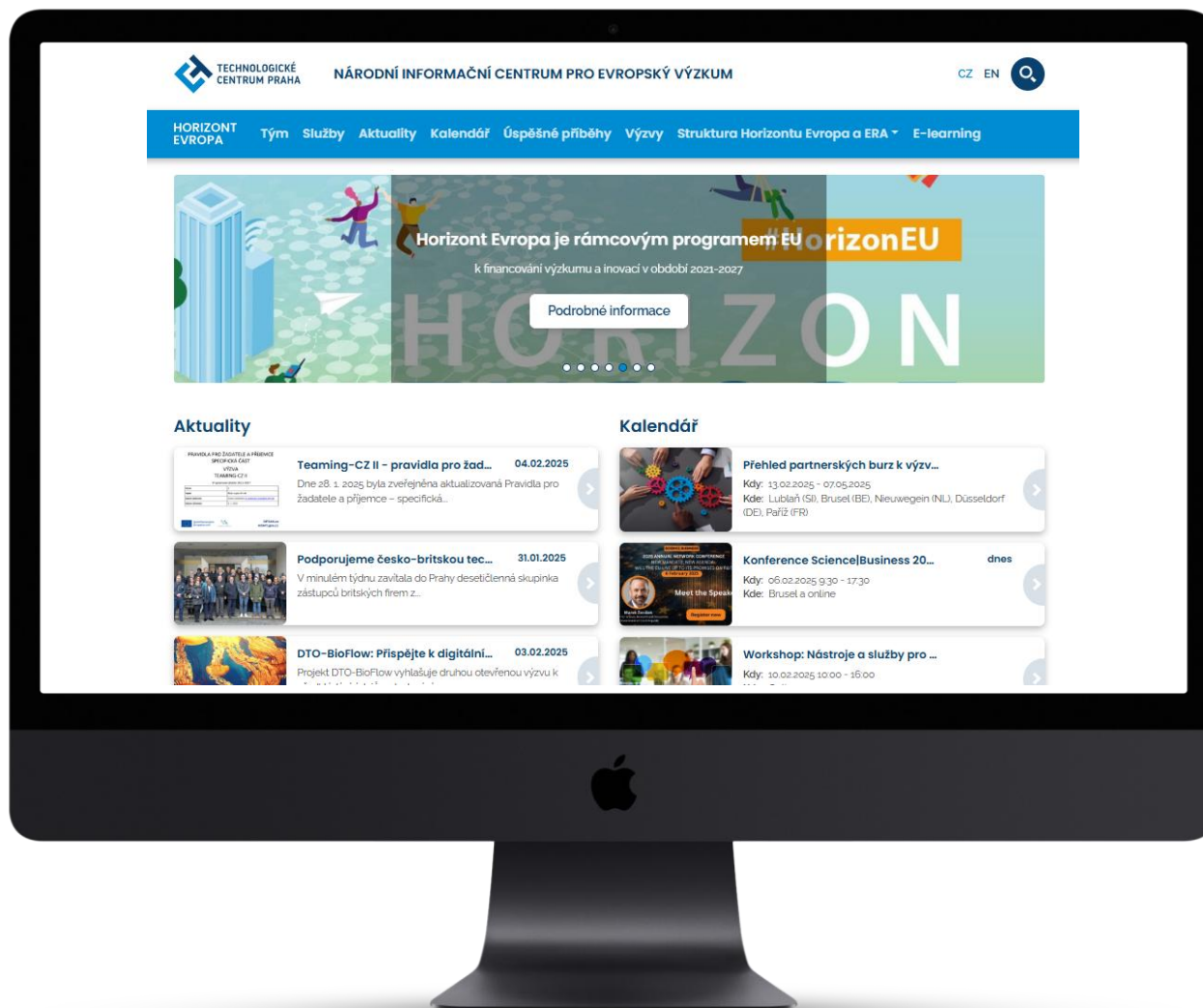
- [Partnerská burza](#) v Paříži v květnu
- [Partnerská burza](#) v Bruselu v červnu
- [Partnerská burza](#) virtuálně v květnu
- Databáze partnerů [SeReMA](#) stále otevřená



PARTNER NEBO KOORDINÁTOR?



Využívejte služby TC Praha <https://www.horizontevropa.cz/cs/nase-sluzby>



VÍCE INFORMACÍ

Národní portál
www.horizontevropa.cz

Kontakty na NCPs (National contact points)
<https://www.horizontevropa.cz/cs/narodni-kontakty>

Měsíční zpravodaj do Vašeho emailu





Lenka Švejcarová

Národní kontakt pro program Horizont Evropa

Klastr 3 – bezpečnost občanů ve společnosti

Klastr 4 – digitalizace, průmysl, vesmír

svejcarova@tc.cz, +420 725 539 546

www.tc.cz

www.horizontevropa.cz